

BEST AVAILABLE COPY

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-219291

(43)Date of publication of application : 10.08.1999

(51)Int.Cl.

G06F 9/06

G06F 12/14

G09C 1/00

H04L 9/10

H04L 9/32

(21)Application number : 10-035484

(71)Applicant : NIPPON CHEMICON CORP

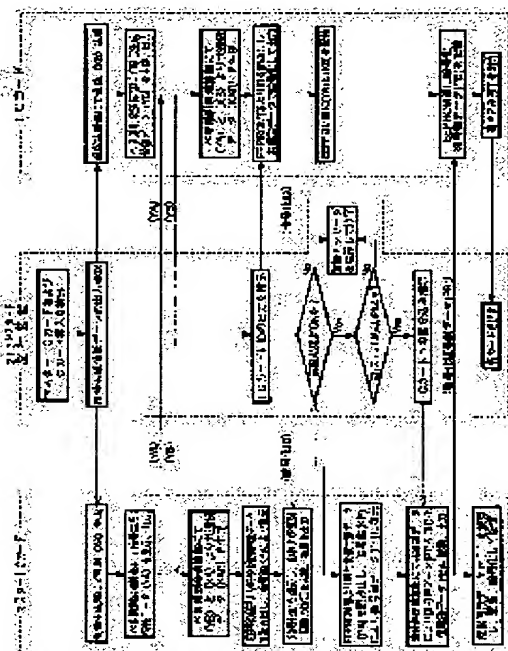
(22)Date of filing : 02.02.1998

(72)Inventor : YAMAMOTO KAZUYUKI

(54) LICENSE CARD MANUFACTURING SYSTEM**(57)Abstract:**

PROBLEM TO BE SOLVED: To provide a license card manufacturing system of for preventing decoding key data from being illegally used by a third person.

SOLUTION: In this manufacture system of the license card for writing the decoding key data from a master IC card for storing at least the decoding key data for decoding ciphered program data and duplication number-of-times data to an IC card and performing duplication, when the decoding key data are written to the IC card, the decoding key data ciphered based on prescribed common key data are outputted from the master IC card. The ciphered decoding key data are restored by the common key data and stored in the IC card and the duplication number-of-times data are subtracted every time the write is executed into the IC card.

**LEGAL STATUS**

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

BEST AVAILABLE COPY

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-219291

(43) 公開日 平成11年(1999) 8月10日

(51) Int.Cl.⁶

G 0 6 F 9/06

識別記号

5 5 0

F I

G 0 6 F 9/06

5 5 0 B

5 5 0 L

12/14

3 2 0

12/14

3 2 0 B

G 0 9 C 1/00

6 6 0

G 0 9 C 1/00

6 6 0 A

H 0 4 L 9/10

H 0 4 L 9/00

6 2 1 A

審査請求 未請求 請求項の数 6 F D (全 11 頁) 最終頁に続く

(21) 出願番号

特願平10-35484

(22) 出願日

平成10年(1998) 2月2日

(71) 出願人 000228578

日本ケミコン株式会社

東京都青梅市東青梅1丁目167番地の1

(72) 発明者 山本 和行

東京都青梅市東青梅一丁目167番地の1

日本ケミコン株式会社内

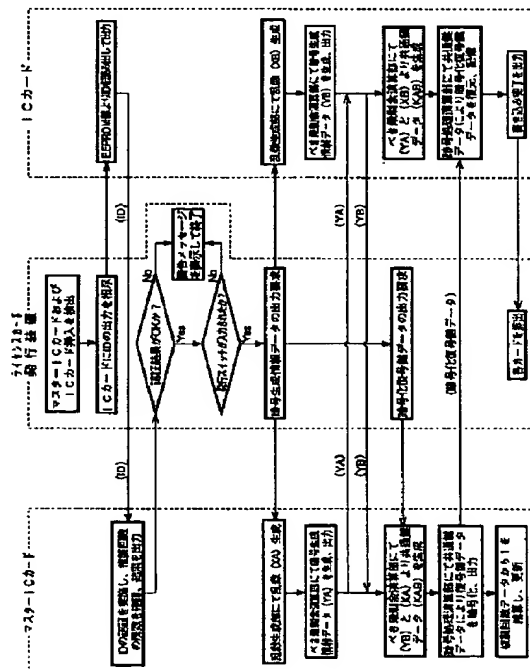
(74) 代理人 弁理士 日高 一樹 (外1名)

(54) 【発明の名称】 ライセンスカードの作製方式

(57) 【要約】

【課題】 第三者によって、復号鍵データが盗用されることのないライセンスカードの作製方式を提供する。

【解決手段】 少なくとも暗号化されたプログラムデータを復号する復号鍵データと複製回数データとを記憶するマスターICカード6より、前記復号鍵データをICカード8に書き込み、複製するライセンスカードの作製方式であって、この復号鍵データがICカード8に書き込まれる際に、前記マスターICカード6から、所定の共通鍵データに基づいて暗号化された復号鍵データが出力され、前記ICカード8には、この暗号化された復号鍵データが共通鍵データにより復元されて記憶され、前記ICカード8に前記書き込みが実施される毎に前記複製回数データが減算されるようにする。



【特許請求の範囲】

【請求項 1】 少なくとも暗号化されたプログラムデータを復号する復号鍵データと複製回数データとを記憶するマスター IC カードより、前記復号鍵データを IC カードに書き込み、複製するライセンスカードの作製方式であって、この復号鍵データが IC カードに書き込まれる際に、前記マスター IC カードから、所定の共通鍵データに基づいて暗号化された復号鍵データが出力され、前記 IC カードには、この暗号化された復号鍵データが共通鍵データにより復元されて記憶され、前記 IC カードに前記書き込みが実施される毎に前記複製回数データが減算されることを特徴とするライセンスカードの作製方式。

【請求項 2】 少なくとも暗号化されたプログラムデータを復号する復号鍵データと複製回数データとを記憶するマスター IC カードより、前記復号鍵データを IC カードに書き込み、複製するライセンスカードの作製方式であって、この復号鍵データが IC カードに書き込まれる際に、前記マスター IC カードから、所定の共通鍵データに基づいて暗号化された復号鍵データが出力され、前記 IC カードに書き込みが実施される毎に前記複製回数データが減算されるとともに、前記 IC カードには、この暗号化された復号鍵データと共通鍵データとが記憶され、必要に応じて暗号化された復号鍵データが前記共通鍵データにより復元されることを特徴とするライセンスカードの作製方式。

【請求項 3】 前記共通鍵データが、IC カードへの書き込みが実施される都度毎に生成されるようになっている請求項 1 または 2 に記載のライセンスカードの作製方式。

【請求項 4】 前記 IC カードに、ID 等の識別データが記憶され、書き込み時に前記マスター IC カードが、この識別データの認証を行うようになっている請求項 1 ～ 3 のいずれかに記載のライセンスカードの作製方式。

【請求項 5】 前記 ID 等の識別データが、IC カードより前記所定の共通鍵データに基づいて暗号化されて出力され、前記マスター IC カードにおいて共通鍵データによって復元されるようになっている請求項 4 に記載のライセンスカードの作製方式。

【請求項 6】 前記マスター IC カードにおいて、各マスター IC カードに固有の ID 等の識別データと、この識別データと対応付けられた暗号鍵データが記憶され、これらマスター IC カードに前記復号鍵データおよび複製回数データが書き込まれる際に、そのマスター IC カードの識別データを読み出し、その識別データに対応する暗号鍵データにより復号鍵データおよび複製回数データが暗号化されて書き込み、記憶され、必要に応じてこの暗号化された復号鍵データおよび複製回数データが前記暗号鍵データによって復元されるようになっている請求項 1 ～ 5 のいずれかに記載のライセンスカードの作製

方式。

【発明の詳細な説明】

【0001】

【発明の属する技術の分野】本発明は、CDROM や DVD 等の記憶媒体に記憶されたゲームソフト等のプログラムデータの不正使用を防止するためのライセンスカードの作製方式に関する。

【0002】

【従来の技術】近年、CDROM や DVD 等の記憶媒体に記憶されたゲームソフト等のプログラムデータを不正にコピーして使用する不正使用が社会的な問題となっている。

【0003】これら不正使用を防止するための方法として、これら CDROM や DVD 等の記憶媒体に記憶されるプログラムデータを暗号化して記憶しておき、これら暗号化されたプログラムデータを復号する復号鍵データ（ライセンス鍵データ）を入手しないと、暗号化されたプログラムデータを平文データに復号することができないようにして、不正なコピーや使用を防止する方法が提案されている。

【0004】しかしながら、これら復号鍵データ（ライセンス鍵データ）を用いた場合においては、暗号化されたプログラムデータそのものを複製しても、そのまま使用することができないようにすることはできるものの、この復号鍵データ（ライセンス鍵データ）が第三者によって盗用、入手されると、容易に不正な使用が可能になってしまうという問題点があるため、これら復号鍵データ（ライセンス鍵データ）を盗用されないように、ユーザーに配布する必要がある。

【0005】これら盗用の問題を解決するために、近年ではこれら復号鍵データ（ライセンス鍵データ）を IC カード等の電子記憶媒体に記憶して、各ユーザーにライセンスカードとして配布し、ユーザーに対して復号鍵データ（ライセンス鍵データ）が不明なようにして、その IC カードがないとプログラムデータを使用できないようにする試みがなされている。

【0006】

【発明が解決しようとする課題】しかしながら、これら IC カードを用いた復号鍵データ（ライセンス鍵データ）の配布方式は、復号鍵データ（ライセンス鍵データ）の盗用を一元的には防止できるものの、通常においてこれらライセンスカードは、各販売店等にて、前記 IC カードに復号鍵データ（ライセンス鍵データ）が書き込まれているため、これら IC カードへの書き込み時に復号鍵データ（ライセンス鍵データ）が盗用される可能性が高いという問題があった。

【0007】よって、本発明は上記した問題点に着目してなされたもので、IC カードへの書き込み時においても第三者によって、復号鍵データ（ライセンス鍵データ）が盗用されることのないライセンスカードの作製方

式を提供することを目的としている。

【0008】

【課題を解決するための手段】前記した問題を解決するために、本発明のライセンスカードの作製方式は、少なくとも暗号化されたプログラムデータを復号する復号鍵データと複製回数データとを記憶するマスターＩＣカードより、前記復号鍵データをＩＣカードに書き込み、複製するライセンスカードの作製方式であって、この復号鍵データがＩＣカードに書き込まれる際に、前記マスターＩＣカードから、所定の共通鍵データに基づいて暗号化された復号鍵データが出力され、前記ＩＣカードには、この暗号化された復号鍵データが共通鍵データにより復元されて記憶され、前記ＩＣカードに前記書き込みが実施される毎に前記複製回数データが減算されることを特徴としている。この特徴によれば、マスターＩＣカードよりＩＣカードに復号鍵データが書き込まれる際に、マスターＩＣカードより出力される復号鍵データが、共通鍵データにより暗号化されて出力されるため、第三者により復号鍵データ自体を盗用されることを防止することができる。

【0009】本発明のライセンスカードの作製方式は、少なくとも暗号化されたプログラムデータを復号する復号鍵データと複製回数データとを記憶するマスターＩＣカードより、前記復号鍵データをＩＣカードに書き込み、複製するライセンスカードの作製方式であって、この復号鍵データがＩＣカードに書き込まれる際に、前記マスターＩＣカードから、所定の共通鍵データに基づいて暗号化された復号鍵データが出力され、前記ＩＣカードに書き込みが実施される毎に前記複製回数データが減算されるとともに、前記ＩＣカードには、この暗号化された復号鍵データと共通鍵データとが記憶され、必要に応じて暗号化された復号鍵データが前記共通鍵データにより復元されることを特徴としている。この特徴によれば、マスターＩＣカードよりＩＣカードに復号鍵データが書き込まれる際に、マスターＩＣカードより出力される復号鍵データが、共通鍵データにより暗号化されて出力されるため、第三者により復号鍵データ自体を盗用されることを防止することができるばかりか、ＩＣカード内部においても復号鍵データが暗号化された状態にて記憶されていることから、仮にＩＣカード内部より暗号化された復号鍵データが読み出されたとしても、第三者により復号鍵データ自体が盗用されることも防止できる。

【0010】本発明のライセンスカードの作製方式は、前記共通鍵データが、ＩＣカードへの書き込みが実施される都度毎に生成されるようになっていたことが好ましい。このようにすれば、ＩＣカードに復号鍵データが書き込まれる都度毎に異なる共通鍵データが生成されるようになり、この共通鍵データにより暗号化される復号鍵データも、その都度毎に異なるものとなることから、より一層第三者が復号鍵データを入手することを困難な

のとすることができ、より高いセキュリティを実現することができる。

【0011】本発明のライセンスカードの作製方式は、前記ＩＣカードに、ＩＤ等の識別データが記憶され、書き込み時に前記マスターＩＣカードが、この識別データの認証を行うようになっていたことが好ましい。このようにすれば、不正なＩＣカードに復号鍵データの書き込みがなされることを防止できる。

【0012】本発明のライセンスカードの作製方式は、前記ＩＤ等の識別データが、ＩＣカードより前記所定の共通鍵データに基づいて暗号化されて出力され、前記マスターＩＣカードにおいて共通鍵データによって復元されるようになっていたことが好ましい。このようにすれば、正規のＩＣカードに記憶されているＩＤ等の識別データが第三者に盗用されて使用されることを防止できる。

【0013】本発明のライセンスカードの作製方式は、前記マスターＩＣカードにおいて、各マスターＩＣカードに固有のＩＤ等の識別データと、この識別データと対応付けられた暗号鍵データが記憶され、これらマスターＩＣカードに前記復号鍵データおよび複製回数データが書き込まれる際に、そのマスターＩＣカードの識別データを読み出し、その識別データに対応する暗号鍵データにより復号鍵データおよび複製回数データが暗号化されて書き込み、記憶され、必要に応じてこの暗号化された復号鍵データおよび複製回数データが前記暗号鍵データによって復元されるようになっていたことが好ましい。このようにすれば、マスターＩＣカード内部に記憶されている復号鍵データおよび複製回数データが、前記暗号鍵データにより暗号化された状態にて記憶、格納されていることから、これらマスターＩＣカードから記憶内容が盗用されたとしても、復号鍵データ自体が第三者に盗用されることを防止できるばかりか、複製回数データ等を改ざんすることによる不正も防止できる。

【0014】

【発明の実施の形態】以下、図面に基づいて本発明の実施形態を説明する。

【0015】（実施例１）図１は、本実施例１における本発明のライセンスカードの作製方式を用いたライセンスカード発行装置の外観を示す外観斜視図であり、図２は本実施例１の前記ライセンスカード発行装置およびマスターＩＣカードとＩＣカードの各構成を示すブロック図であり、図３（ａ）は、本実施例１のマスターＩＣカードに用いた暗号処理部の構成および処理内容を示すブロック図であり、図３（ｂ）は、本実施例１のＩＣカードに用いた暗号処理部の構成および処理内容を示すブロック図であり、図４は、本実施例１のライセンスカード発行装置およびマスターＩＣカードとＩＣカードとの処理動作を示す図である。

【0016】本実施例１は、本発明のライセンスカード

の作製方式をライセンスカード発行装置に応用したものである。

【0017】本実施例のライセンスカード発行装置1は、図1に示されるような外観を有しており、マスターICカード6を挿入するマスターICカードリーダライタ2と、復号鍵データ(ライセンス鍵データ)が書き込まれてライセンスカードとして発行されるICカード8を挿入するICカードリーダライタ3が前面部に設けられ、その上部には、動作状況やメッセージ等を表示する表示部4と、復号鍵データの書き込みを実施させる発行スイッチ5が設けられている。

【0018】これらマスターICカード6およびICカード8およびライセンスカード発行装置1の構成は、図2に示される様になっており、前記マスターICカード6にはIC7が内蔵されており、このIC7の内部には、前記復号鍵データおよび複製回数を記憶する記憶手段として、不揮発性メモリであるEEPROM部14と、各種演算等において使用されるメモリ部15と、後述する所定のアルゴリズムに基づき暗号生成情報データおよび共通鍵データの生成と復号鍵データの暗号化を実施する暗号生成部16と、前記マスターICカードリーダライタ2とのデータのやり取りを実施する通信部13と、これら各部の制御等を実施する制御部12が設けられており、本実施例1では前記EEPROM部14に、復号鍵データの書き込みがなされる正規のICカードに付与されているIDが予め記憶されている。

【0019】また、前記ICカード8にはIC9が内蔵されており、これらICカード8には、本実施例1では固有のIDが付与されており、前記IC9の内部には、後述する暗号生成部21により復元された復号鍵データや前記ID等を記憶する不揮発性メモリであるEEPROM部19と、各種演算等において使用されるメモリ部20と、後述する所定のアルゴリズムに基づき暗号生成情報データおよび共通鍵データの生成と暗号化された復号鍵データの復元を実施する暗号生成部21と、前記ICカードリーダライタ3とのデータのやり取りを実施する通信部17と、これら各部の制御等を実施する制御部18が設けられており、前記EEPROM部19にはICカード8に付与されたIDデータが予め記憶されている。

【0020】また、ライセンスカード発行装置1には、前記マスターICカードリーダライタ2とICカードリーダライタ3と表示部としてのLCDパネル4と、このLCDパネル4の表示動作を制御するLCDドライバ11と、発行スイッチ5と、これら各部の制御を実施するマイクロプロセッシングユニット(MPU)10が設けられ、前記MPU10の内部には内部ROM(図示せず)が設けられ、MPU10が行う制御動作が記述されたプログラムが予め記憶、格納されている。

【0021】また、前記IC7に内蔵されている暗号生

成部16は、図3(a)に示されるようなプロセスを備える構成とされ、乱数生成部によって生成された乱数

(XA)に基づいて、べき乗剰余演算部により所定長の暗号生成情報データ(YA)がべき乗剰余演算により生成されるようになっており、この暗号生成部16により生成された暗号生成情報データ(YA)は、通信部13およびマスターICカードリーダライタ2、ライセンスカード発行装置1、ICカードリーダライタ3を介してICカード8に出力されるとともに、このICカード8からも、図3(b)に示すように、IC9に内蔵されている暗号生成部21により前記暗号生成部16と同様のアルゴリズムによって生成された暗号生成情報データ

(YB)が出力されて、前記暗号生成部16のべき乗剰余演算部に入力され、これら暗号生成情報データ(YB)と前記乱数生成部によって生成された乱数(XA)とが、べき乗剰余演算部によりべき乗剰余演算されることにより共通鍵データ(KAB)が生成されるようになっており、この共通鍵データ(KAB)に基づいて、前記EEPROM部14に記憶されている復号鍵データが暗号処理演算部により暗号化されるようになっている。

【0022】また、前記ICカード8のIC9に内蔵されている暗号生成部21は、図3(b)に示されるように、前記暗号生成部16と同様のプロセスを備える構成とされており、乱数生成部によって生成された乱数(XB)に基づいて、べき乗剰余演算部により所定長の暗号生成情報データ(YB)がべき乗剰余演算により生成されて、ICカード8よりライセンスカード発行装置1を介してマスターICカード6に出力されるようになっており、前記暗号生成部16同様に、マスターICカード6の暗号生成部16より生成、出力された暗号生成情報データ(YA)が、暗号生成部21のべき乗剰余演算部に入力され、この暗号生成情報データ(YA)と前記乱数生成部によって生成された乱数(XB)とが、べき乗剰余演算部によりべき乗剰余演算されることにより前記暗号生成部16において生成された共通鍵データ(KAB)と同一の共通鍵データ(KAB)が生成されるようになっており、この共通鍵データ(KAB)に基づいて、暗号化された復号鍵データが、暗号処理演算部にて復元されるようになっている。

【0023】これらマスターICカード6とライセンスカード発行装置1とICカード8との間におけるデータ等のやり取りは、図4に示されるようになっており、マスターICカード6とICカード8とがライセンスカード発行装置1に挿入されると、これら各カードの挿入が検出され、ICカード8に対してIDデータを出力するように、ライセンスカード発行装置1のMPU10が指示を出力する。

【0024】この出力に基づいて、ICカード8のIC9に内蔵されている制御部18は、前記EEPROM部19に予め記憶されているIDデータを読み出し、通信

部 17 およびライセンスカード発行装置 1 を介してマスター IC カード 6 に出力する。

【0025】この ID データの出力を受けて、マスター IC カード 6 の IC 7 に内蔵されている制御部 12 は、この ID データを EEPROM 部 14 に予め記憶されている ID データから検索、比較して認証を実施するとともに、複製回数に残数が存在するかを確認し、その認証結果をライセンスカード発行装置 1 に出力する。

【0026】前記 MPU 10 は、この認証結果が「否」である場合には、書き込みがなされる IC カード 8 が正規のものでないことを前記 LCD パネル 4 に表示して、処理を終了し、認証結果が「可」である場合には、LCD パネル 4 に「発行スイッチを押して下さい」のメッセージを表示し、発行スイッチ 5 の入力待ちを所定時間行い、所定時間内に発行スイッチ 5 が入力されない場合には、各カードを排出して、処理を終了する。

【0027】前記所定時間内に発行スイッチ 5 が入力された場合には、MPU 10 は、共通鍵データを生成するための暗号生成情報データの出力をマスター IC カード 6 および IC カード 8 に指示する。

【0028】この指示を受けて、マスター IC カード 6 および IC カード 8 の各制御部 12、18 は、暗号生成部 16、21 に暗号生成情報データの生成を指示し、暗号生成部 16、21 においては、前記したように、乱数生成部において乱数 (XA)、(XB) が生成され、これがべき乗剰余演算部においてべき乗剰余演算されて暗号生成情報データ (YA)、(YB) が生成されて、各制御部 12、18 に出力され、各制御部 12、18 は、これら暗号生成情報データ (YA)、(YB) を通信部 13、17 およびライセンスカード発行装置 1 を介して IC カード 8 およびマスター IC カード 6 に出力する。

【0029】これら各出力された暗号生成情報データ (YB)、(YA) は、マスター IC カード 6 および IC カード 8 の各暗号生成部 16、21 に入力され、各べき乗剰余演算部において、前記各乱数生成部において生成された乱数 (XA)、(XB) とべき乗剰余演算されて共通鍵データ (KAB) が生成される。

【0030】前記 MPU 10 は、これら暗号生成情報データ (YA)、(YB) の出力に次いで、マスター IC カード 6 に暗号化された復号鍵データの出力要求を出力し、マスター IC カード 6 の制御部 12 は、この指示に基づいて前記にて生成された共通鍵データ (KAB) により、暗号処理演算部にて前記 EEPROM 部 14 より読み出した復号鍵データの暗号化を実施させ、暗号化された復号鍵データを、ライセンスカード発行装置 1 を介して IC カード 8 に出力するとともに、EEPROM 部 14 に記憶されている複製回数データより 1 を減じて複製回数データを更新する。

【0031】このようにして出力された暗号化された復号鍵データは、IC カード 8 の暗号生成部 21 に入力さ

れ、前記にて生成された共通鍵データ (KAB) により暗号処理演算部にて復号鍵データに復元され、復元された復号鍵データが前記 EEPROM 部 19 に記憶される。

【0032】これら復号鍵データの復元、記憶が完了すると、IC カード 8 の制御部 18 は、ライセンスカード発行装置 1 に復号鍵データの書き込みが完了したことを出力し、この出力に基づいて MPU 10 は、各カードの排出を実施して処理を終了する。

【0033】また、本実施例 1 においては、前記したように共通鍵データが IC カード 8 への書き込みが実施される都度毎に、暗号生成情報データが交換されることにより異なる共通鍵データが生成されるようになっているが、本発明はこれに限定されるものではなく、これら共通鍵データが固定またはマスター IC カードや IC カード毎に固定の暗号生成情報データが割り当てられたものとしても良いが、本実施例 1 のようにすれば、その都度異なる共通鍵データが生成されて、この共通鍵データによって暗号化される復号鍵データも異なるようになることから、第三者がこれら復号鍵データを盗用することにより困難なものとすることができ、より高いセキュリティを実現できることから好ましい。

【0034】(実施例 2) 図 5 (a) および (b) は、本実施例 2 におけるマスター IC カード 6 の IC 7 に内蔵される暗号生成部 16' の構成および処理内容を示すブロック図であり、図 6 は、本実施例 2 における IC カード 8 の IC 9 に内蔵される暗号生成部 21' の構成および処理内容を示すブロック図であり、図 7 は、本実施例 2 のライセンスカード発行装置 1 およびマスター IC カード 6 と IC カード 8 との処理動作を示す図である。

【0035】本実施例 2 の構成は、前記実施例 1 とほぼ同様の構成とされているが、その特徴としては、前記マスター IC カード 6 の EEPROM 部 14 に記憶されている復号鍵データが、暗号化された状態にて記憶されているとともに、IC カード 8 より出力される ID データが、共通鍵データにより暗号化されて出力されるようになっている点が大きく異なり、これら暗号化された復号鍵データを復元したり ID データを暗号化するために、マスター IC カード 6 および IC カード 8 の各暗号生成部 16、21 が図 5 および図 6 に示されるような各暗号生成部 16'、21' に変更されているとともに、ライセンスカード発行装置 1 の MPU 10 内部に設けられている内部 ROM (図示せず) のプログラムも変更されている。

【0036】本実施例 2 において使用されるマスター IC カード 6 には、予め固有の識別符号である ID が付与され、この ID と ID に関連付けられた暗号鍵データとが、EEPROM 部 14 に予め記憶されている。

【0037】これらマスター IC カード 6 に復号鍵データ (PT) および複製回数データが書き込まれる際にお

いては、マスターICカード6の前記IDデータが読み出され、このIDに関連付けられた暗号鍵データ(KP)により復号鍵データ(PT)および複製回数データが所定のアルゴリズムに基づき暗号化されて書き込まれ、この暗号化復号鍵データ(PA)および暗号化複製回数データがEEPROM部14に記憶されている。

【0038】これに伴い、マスターICカード6のIC7に内蔵されている暗号生成部16'は、図5(a)に示すように、EEPROM部14に記憶されている暗号鍵データ(KP)に基づき暗号処理演算部にて暗号化復号鍵データ(PA)および暗号化複製回数データが復号鍵データ(PT)および複製回数データに復元されるようになっており、また図5(b)に示すように、ICカード8より出力される共通鍵データ(KAB)により暗号化された暗号化IDデータが、共通鍵データ(KAB)によりIDデータに復元されるようになっている。

【0039】また、ICカード8のIC9に内蔵されている暗号生成部21'も、図6に示されるように、前記実施例1の暗号生成部21の処理に加えて、ICカード8のEEPROM部19に記憶されている各ICカードのIDデータが、共通鍵データ(KAB)により暗号化IDデータに変換されるようになっている。

【0040】本実施例2におけるマスターICカード6とライセンスカード発行装置1とICカード8との間におけるデータ等のやり取りは、図7に示されるようになっており、マスターICカード6とICカード8とがライセンスカード発行装置1に挿入されると、これら各カードの挿入が検出され、まずマスターICカード6とICカード8とに、暗号生成情報データの出力要求をライセンスカード発行装置1のMPU10が出力する。

【0041】この出力に基づいて、マスターICカード6およびICカード8の各制御部12、18は、前記実施例1と同様に暗号生成情報データ(YA)、(YB)の生成を各暗号生成部16'、21'に指示し、生成された暗号生成情報データ(YA)、(YB)をライセンスカード発行装置1を介してICカード8およびマスターICカード6に出力し、これら出力された暗号生成情報データ(YA)、(YB)に基づいて共通鍵データ(KAB)が生成される。

【0042】次いでMPU10は、ICカード8にIDデータの出力を指示し、この指示によって、ICカード8の制御部18は、暗号生成部21'にEEPROM部19より読み出したIDデータの暗号化を共通鍵データ(KAB)に基づいて実施するように指示し、この暗号化された暗号化IDデータをライセンスカード発行装置1を介してマスターICカード6に出力する。

【0043】マスターICカード6では、この暗号化IDデータを前記したように暗号生成部16'に入力し、共通鍵データ(KAB)により復元してIDデータとするとともに、EEPROM部14より暗号化複製回数デ

ータを読み出し、これを暗号鍵データ(KP)により複製回数データに復元し、前記復元されたIDデータおよび複製回数データを実施例1と同様にして認証を実施し、その結果をライセンスカード発行装置1に出力するとともに、その認証結果が「可」である場合には、EEPROM部14に暗号化された状態にて記憶されている暗号化復号鍵データ(PA)の復元を暗号生成部16'に指示し、前記EEPROM部14に記憶されている暗号鍵データ(KP)に基づいて、暗号処理演算部にて復号鍵データ(PT)が復元される。

【0044】前記MPU10は、この認証結果が「否」である場合には、書き込みがなされるICカード8が正規のものでないことを前記LCDパネル4に表示して、処理を終了し、認証結果が「可」である場合には、LCDパネル4に「発行スイッチを押して下さい」のメッセージを表示し、発行スイッチ5の入力待ちを所定時間行い、所定時間内に発行スイッチ5が入力されない場合には、各カードを排出して、処理を終了する。

【0045】前記所定時間内に発行スイッチ5が入力された場合には、MPU10は、マスターICカード6に暗号化復号鍵データ(PB)の出力を要求する。

【0046】この出力により制御部12は、前記にて復元した復号鍵データ(PT)を共通鍵データ(KAB)に基づき暗号化する指示を暗号生成部16'に出し、これにより暗号化された暗号化復号鍵データ(PB)をライセンスカード発行装置1を介してICカード8に出力するとともに、前記複製回数データより1を減算して更新し、これを前記暗号鍵データ(KP)に基づいて暗号化してEEPROM部14にお再度記憶する。

【0047】ICカード8では、この暗号化復号鍵データ(PB)をEEPROM部19に記憶するとともに、前記暗号生成情報データ(YA)、と乱数データ(XB)とを記憶し、ICカード8の制御部18は、ライセンスカード発行装置1に復号鍵データの書き込みが完了したことを出力し、この出力に基づいてMPU10は、各カードの排出を実施して処理を終了する。

【0048】これらICカード8のEEPROM部19に記憶された暗号化復号鍵データ(PB)は、暗号生成部21'により、必要に応じて共通鍵データ(KAB)により復号鍵データ(PT)に復元されて使用される。

【0049】本実施例2のようにすれば、マスターICカードおよびICカードの記憶手段であるEEPROMに復号鍵データが暗号化された状態にて記憶され、必要に応じて復元されて使用されることとなり、マスターICカードおよびICカードより復号鍵データ自体が盗用されることを防止できるばかりか、ICカードから出力されるIDデータも共通鍵データにより暗号化されて出力されるようになることから、これらIDデータが第三者に不正に盗用されて不正なICカードに復号鍵データが複製されることを防止できるようになる。

10

20

30

40

50

【0050】また、本実施例2においては、前記EEPROM部19に暗号生成情報データ(YA)、と乱数データ(XB)とを記憶しているが、これを共通鍵データ(KAB)自体を記憶しても良いが、本実施例のように暗号生成情報データ(YA)、と乱数データ(XB)とを記憶することにより、共通鍵データ(KAB)自体が読み出されて暗号化復号鍵データ(PB)が復元されることを防止できることから好ましい。

【0051】また、本実施例2においては、暗号鍵データにより暗号化された暗号化復号鍵データ(PA)を暗号生成部において、共通鍵データによる暗号化と同様のアルゴリズムを用いて暗号化および復元を実施しているが、本発明はこれに限定されるものではなく、これら暗号化復号鍵データ(PA)を共通鍵データによる暗号化と異なるアルゴリズムを用いても良いが、本実施例2のように共通化することにより、機器構成を簡略化することができることから好ましい。

【0052】以上、本発明を図面に基いて説明してきたが、本発明はこれら各実施例に限定されるものではなく、本発明の主旨を逸脱しない範囲での変更や追加があっても、本発明に含まれることは言うまでもない。

【0053】また、本実施例では、共通鍵データを暗号生成情報データを交換することにより生成しているが、本発明はこれに限定されるものではなく、その他の方法、例えば、乱数生成のための初期値データを交換したりして共通鍵データを生成するようにしても良い。

【0054】また、本実施例においては、復号鍵データを不揮発性のEEPROM部に記憶しているが、本発明はこれに限定されるものではなく、この復号鍵データをその他の不揮発性メモリ、例えば強誘電体メモリ(F e RAM)、フラッシュメモリ等に記憶させても良い。

【0055】

【発明の効果】本発明は次の効果を奏する。

【0056】(a) 請求項1の発明によれば、マスターICカードよりICカードに復号鍵データが書き込まれる際に、マスターICカードより出力される復号鍵データが、共通鍵データにより暗号化されて出力されるため、第三者により復号鍵データ自体を盗用されることを防止することができる。

【0057】(b) 請求項2の発明によれば、マスターICカードよりICカードに復号鍵データが書き込まれる際に、マスターICカードより出力される復号鍵データが、共通鍵データにより暗号化されて出力されるため、第三者により復号鍵データ自体を盗用されることを防止することができるばかりか、ICカード内部においても復号鍵データが暗号化された状態にて記憶されていることから、仮にICカード内部より暗号化された復号鍵データが読み出されたとしても、第三者により復号鍵データ自体が盗用されることも防止できる。

【0058】(c) 請求項3の発明によれば、ICカー

ドに復号鍵データが書き込まれる都度毎に異なる共通鍵データが生成されるようになり、この共通鍵データにより暗号化される復号鍵データも、その都度毎に異なるものとなることから、より一層第三者が復号鍵データを入力することを困難なものとしことができ、より高いセキュリティを実現することができる。

【0059】(d) 請求項4の発明によれば、不正なICカードに復号鍵データの書き込みがなされることを防止できる。

【0060】(e) 請求項5の発明によれば、正規のICカードに記憶されているID等の識別データが第三者に盗用されて使用されることを防止できる。

【0061】(f) 請求項6の発明によれば、マスターICカード内部に記憶されている復号鍵データおよび複製回数データが、前記暗号鍵データにより暗号化された状態にて記憶、格納されていることから、これらマスターICカードから記憶内容が盗用されたとしても、復号鍵データ自体が第三者に盗用されることを防止できるばかりか、複製回数データ等を改ざんすることによる不正も防止できる。

【0062】

【図面の簡単な説明】

【図1】実施例1における本発明のライセンスカードの作製方法を用いたライセンスカード発行装置の外観を示す外観斜視図である。

【図2】本発明の実施例1におけるライセンスカード発行装置およびマスターICカードとICカードの各構成を示すブロック図である。

【図3】(a) 本発明の実施例1におけるマスターICカードに用いた暗号処理部の構成および処理内容を示すブロック図である。

(b) 本発明の実施例1におけるICカードに用いた暗号処理部の構成および処理内容を示すブロック図である。

【図4】本発明の実施例1におけるライセンスカード発行装置およびマスターICカードとICカードとの処理動作を示す図である。

【図5】(a)、(b) 本発明の実施例2におけるマスターICカードのICに内蔵される暗号生成部の構成および処理内容を示すブロック図である。

【図6】本発明の実施例2におけるICカードのICに内蔵される暗号生成部の構成および処理内容を示すブロック図である。

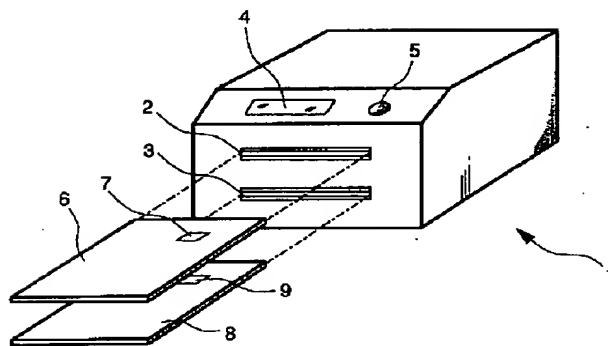
【図7】本発明の実施例2におけるライセンスカード発行装置およびマスターICカードとICカードとの処理動作を示す図である。

【符号の説明】

- | | |
|---|-----------------|
| 1 | ライセンスカード発行装置 |
| 2 | マスターICカードリーダライタ |
| 3 | ICカードリーダライタ |

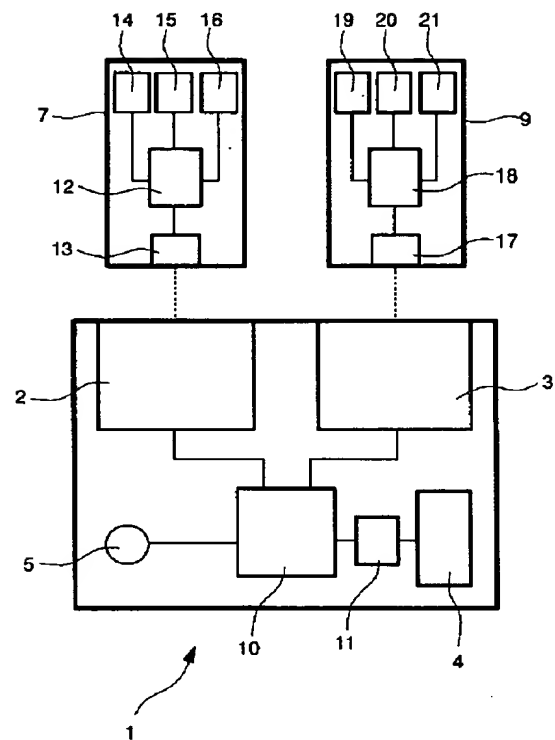
- 13
- 4 LCDパネル
 - 5 発行スイッチ
 - 6 マスターICカード
 - 7 IC
 - 8 ICカード
 - 9 IC
 - 10 マイクロプロセッシングユニット (MPU)
 - 11 LCDドライバ
 - 12 制御部
 - 13 通信部

【図1】

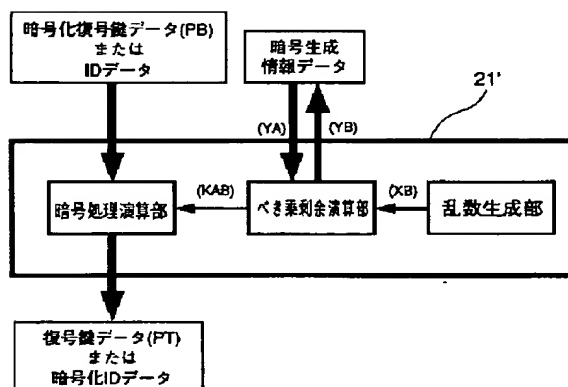


- 14
- 14 EEPROM部
 - 15 メモリ部
 - 16 暗号生成部
 - 16' 暗号生成部
 - 17 通信部
 - 18 制御部
 - 19 EEPROM部
 - 20 メモリ部
 - 21 暗号生成部
 - 10 21' 暗号生成部

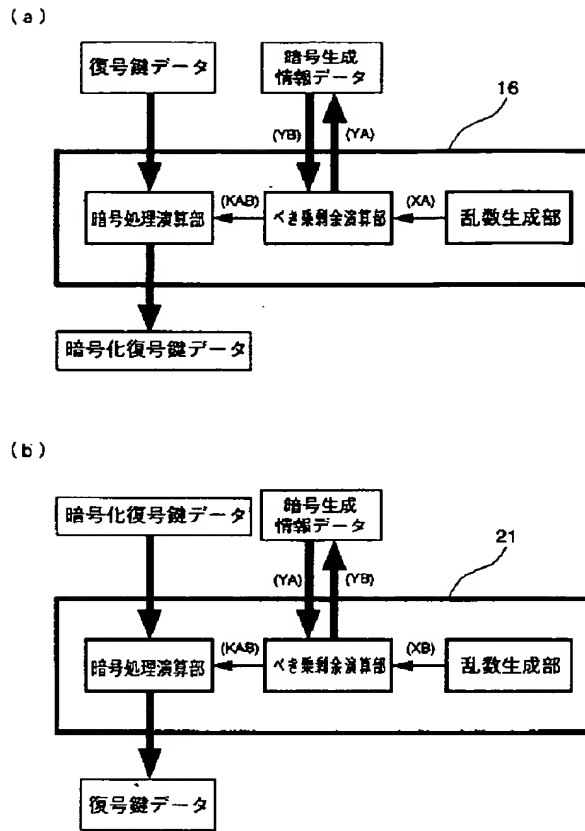
【図2】



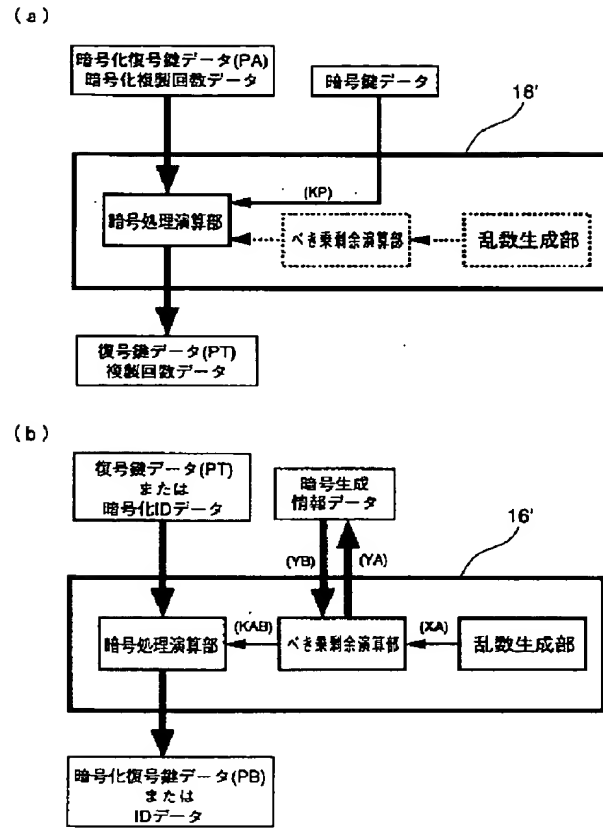
【図6】



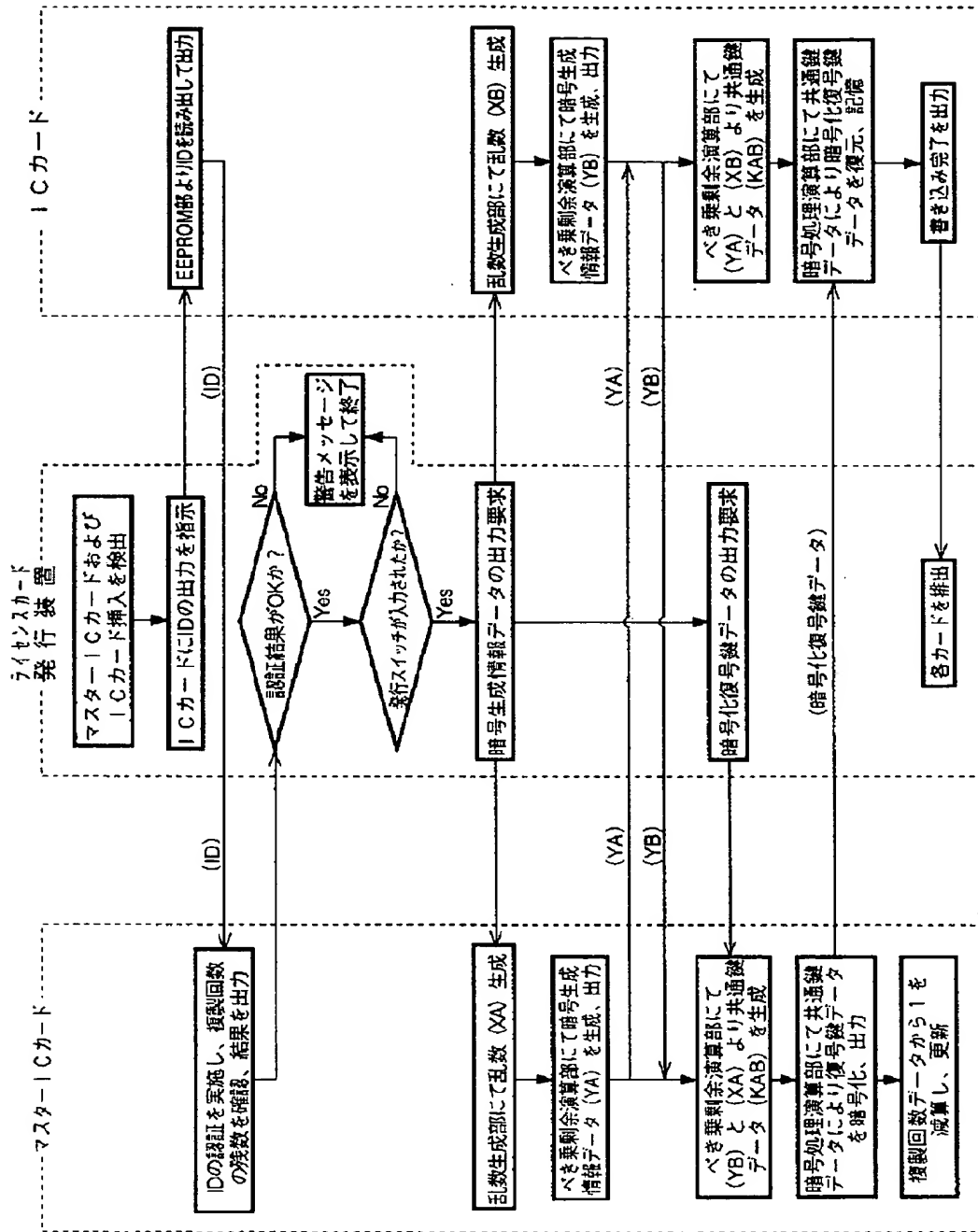
【図3】



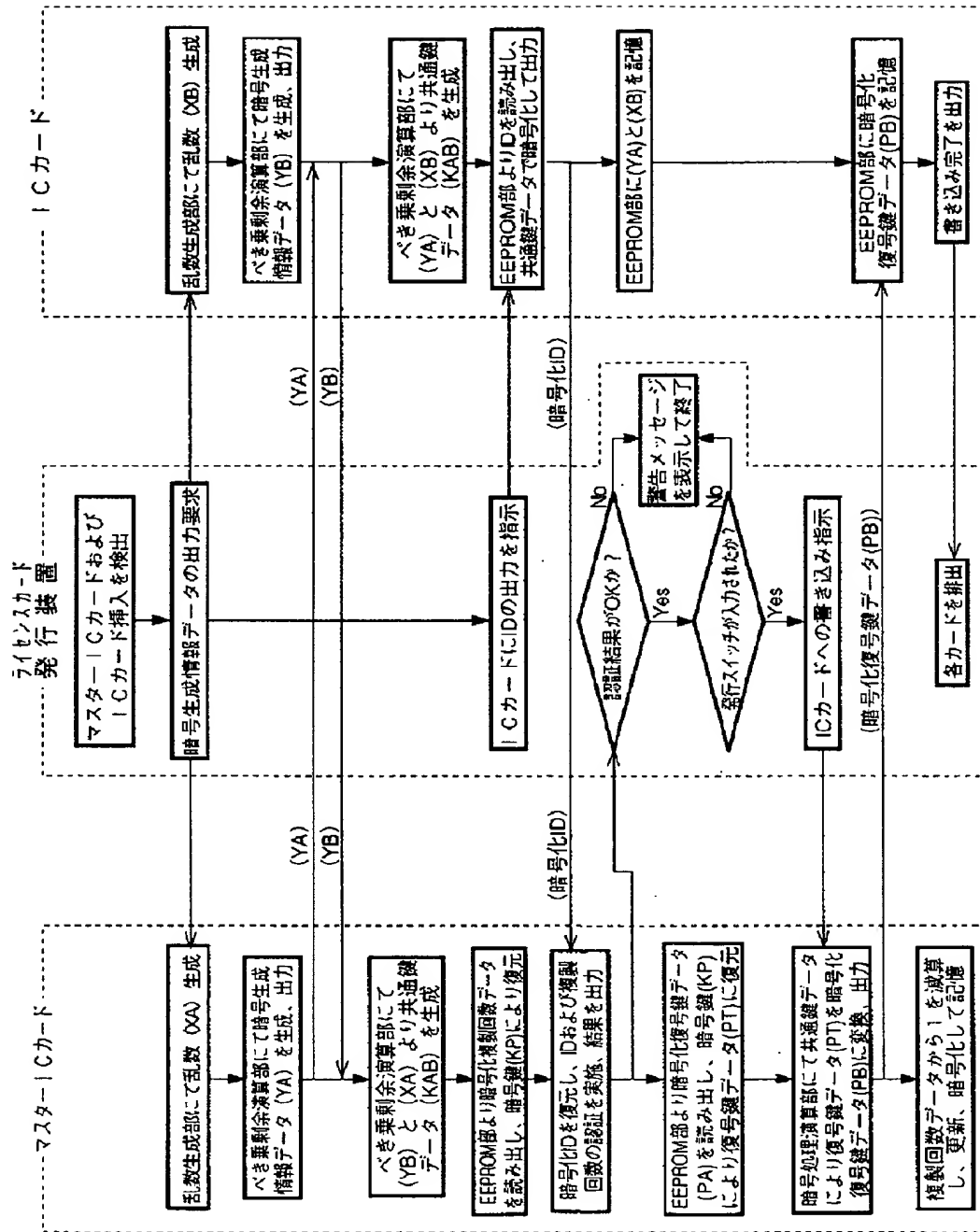
【図5】



【図4】



【図7】



フロントページの続き

(51) Int. Cl. 6

H04L 9/32

識別記号

FI

H04L 9/00

673E

673C